On the Construction of Intransitive Groups.

BY OSKAR BOLZA.

If a substitution-group I is *intransitive*, the letters upon which it operates can be distributed into "*systems of intransitivity,*"

$$x_1, x_2 \ldots ; y_1, y_2 \ldots ; z_1, z_2 \ldots ; \ldots$$

such that the substitutions of I interchange among each other only the letters $x_1, x_2 \ldots$; the letters $y_1, y_2 \ldots$; the letters $z_1, z_2 \ldots$, and so on, and connect transitively the letters of each system. Every substitution of I is then a product $g.h.k\ldots$, g being a substitution between the letters x only, h a substitution between the y, and so on. The substitutions g which occur in the different substitutions of I form together a transitive group G, likewise the h form a group H, and so on.* We will agree, for shortness, to call these groups G, H, $K \ldots$ the *transitive constituents* of the intransitive group I, and we propose to solve, in the present paper, the inverse problem:

Given the transitive substitution-groups G, H, $K \ldots$ between the letters $x_1, x_2 \ldots$; $y_1, y_2 \ldots$; $z_1, z_2 \ldots$; $\ldots$ respectively, to find ALL *the intransitive groups with the systems of intransitivity, $x_1, x_2 \ldots$; $y_1, y_2 \ldots$; $z_1, z_2 \ldots$; $\ldots$, and whose transitive constituents are the groups G, H, $K \ldots$*

There exists always *one self-evident* solution of this problem, viz. the group generated by multiplying by each other, in all possible ways, the substitutions of G, H, $K \ldots$; but there *may* be still other solutions. For instance, if we choose for G the symmetrical group of three letters, for H the symmetrical group of three other letters, it is easily seen that we obtain intransitive groups with the transitive constituents G and H:

a) by multiplying every substitution of G by every substitution of H (order 36);

* Camille Jordan: Traité des substitutions, No. 44.

b) by multiplying every positive (gerade) substitution of G by every positive substitution of H, and every negative substitution of G by every negative substitution of H (order 18);

c) by multiplying every substitution of G by the same substitution of H, that is to say, 1 by 1, (x_1, x_2, x_3) by (y_1, y_2, y_3), (x_1, x_2) by (y_1, y_2), and so on (order 6).

§1.

Reduction of the Problem.

1. The case of more than two systems of intransitivity may successively be reduced to the case of only two systems. For by combining several systems of intransitivity in one larger system, we can always distribute the letters into two systems, $x_1, x_2 \dots$ and $y_1, y_2 \dots$, such that the substitutions of I never replace any of the x by any of the y, nor vice versa. We may then deal with these two systems exactly as we did with the systems of intransitivity; the only difference will be that the groups G and H to which we arrive may now themselves be intransitive, but at any rate they possess *a smaller number of systems of intransitivity* than the original intransitive group. We may therefore confine ourselves to the case of two systems of intransitivity, provided we drop the supposition that the constituent groups G and H are transitive.

The example given above exhibits the two extreme types of intransitive groups: in the first group every substitution of G occurs multiplied *by every one* of the substitutions of H, and vice versa; in the last group, each substitution of G occurs multiplied only *by one single* substitution of H, and vice versa. The object of this § is to *reduce the construction of any intransitive group to these two extreme cases.*

2. Let us then suppose we have found an intransitive group I with the given transitive constituents G and H:

$$I = [gh, g'h', g''h'', \dots].$$

Let
$$l_1 . 1, \ l_2 . 1, \dots \ l_\lambda . 1 \tag{1}$$

be those substitutions of I in which the second factor, h, is unity; they form a group L, since the product* $l . 1 \times l' . 1 = ll' . 1$ belongs again to the substitutions

*I may remark that I use, throughout, Jordan's notations; accordingly, in a product the *left-hand* factor is to be applied *first*. Further small characters shall always represent substitutions which belong to the group represented by the corresponding large character.

(1). This group L *is a self-conjugate subgroup* of* G *as well as of* I; for since every substitution of G is commutative† to every substitution of H, the substitution $(gh)^{-1}$ (which is generally equal to $h^{-1}g^{-1}$) may be written $g^{-1}h^{-1}$, and the transformed of $l.1$ by any substitution gh of I, viz. $(gh)^{-1}l.1\,(gh) = g^{-1}lg.1$, is again one of the substitutions (1).

If gh be any of the substitutions of I, $lg.h$ will also belong to I; and conversely, *if* gh *and* $g'h$ *be two substitutions of* I *with the same factor* h, *then* $g' = lg$; for $g'h \times (gh)^{-1} = g'g^{-1}.1$ belongs to I and in particular to L, therefore $g'g^{-1} = l$ or $g' = lg$.

In like manner the substitutions of I in which the first factor, g, is unity, and which we denote by

$$1.m_1,\ 1.m_2,\ \ldots .\ 1.m_\mu \qquad (2)$$

form a group M, self-conjugate in H as well as in I. And if gh and gh' be two substitutions of I with the same factor g, then $h' = mh$.

If l and m be any substitutions of L resp. M, their product $l.m$ will be a substitution of I, and since the substitutions of L are commutative to those of M and both groups have no common substitutions besides unity, the $\lambda.\mu$ products, $l_\alpha m_\beta$ $(\alpha = 1, 2 \ldots . \lambda;\ \beta = 1, 2 \ldots . \mu)$ are all different and form a group J.‡ J *is a self-conjugate subgroup of* I; for $(gh)^{-1}lm\,(gh) = g^{-1}lg.h^{-1}mh$, and this may be written $l'm'$, since L is self-conjugate in G and M self-conjugate in H.

If in a substitution gh *of* I *the first factor* g *belongs to* L, *then the second,* h, *will belong to* M *and therefore* gh *to* J. For by multiplying $l.h$ by $l^{-1}.1$, which is sure to belong to I, we see that $1.h$ is a substitution of I and especially of M, therefore $h = m$. Similarly, if the second factor of gh belongs to M, then the first will belong to L.

3. Applying a well-known theorem to the group I and its subgroup J, we exhibit the substitutions of I, whose order we suppose to be r, in the form $l_\alpha m_\beta i_\gamma$, $\alpha = 1, 2 \ldots . \lambda$; $\beta = 1, 2 \ldots . \mu$; $\gamma = 1, 2 \ldots . \varkappa = \dfrac{r}{\lambda\mu}$, the multipliers $i_1 = 1, i_2 \ldots . i_\kappa$ being substitutions of I, subject to the only condition that, if α and β be different, then $i_\beta i_\alpha^{-1}$ shall not belong to the subgroup J.

---

* "Ausgezeichnete Untergruppe." See Cole "On Klein's Icosaeder," *Amer. Jour. Math.*, Vol. IX.

† "Per mutable à."

‡ See Serret, Cours d'Algèbre, No. 435.

We decompose the substitutions i_γ into factors g and h and denote them by

$$g_1h_1 = 1,\; g_2h_2,\; \ldots\ldots\; g_\kappa h_\kappa. \tag{3}$$

The $r = \lambda\mu\kappa$ substitutions of I may then be written $l_\alpha g_\gamma . m_\beta h_\gamma$, the indices taking the above indicated values.

Since G is supposed to be a transitive constituent of I, the $\lambda\kappa$ substitutions $l_\alpha g_\gamma$ must all belong to G, and each substitution of G must be found among them. I say these $\lambda\kappa$ substitutions are all different. For if $l_\alpha g_\gamma$ were equal to $l_{\alpha'} g_{\gamma'}$, we should obtain a relation $g_{\gamma'} = lg_\gamma$; but then the product $i_{\gamma'} i_\gamma^{-1}$ would be equal to $l . h_{\gamma'} h_\gamma^{-1}$ and would, according to No. 2, end, belong to J, against our assumption about the i_γ. Therefore *the $\lambda\kappa$ substitutions $l_\alpha g_\gamma$ are all different and represent all the substitutions of G and each one only once;* therefore the order p of G is $\lambda\kappa$.

Similarly the $\mu\kappa$ substitutions $m_\beta h_\gamma$ are all different and represent exactly the group H, whose order q is consequently $\mu\kappa$. Hence follows the theorem:

Between the orders p, q, λ, μ of the groups G, H, L, M resp. exists the relation

$$\frac{p}{\lambda} = \frac{q}{\mu} = \kappa. \tag{4}$$

4. The substitutions $g_1, g_2, \ldots\ldots g_\kappa$ do not, as a rule, form a group; but we can introduce κ substitutions $\mathfrak{g}_1, \mathfrak{g}_2 \ldots\ldots \mathfrak{g}_\kappa$ corresponding to them which form a group. In the analytical representation of substitutions of p letters, it is usual to agree that the same letter x_z may also be represented by $x_{z+p}, x_{z+2p} \ldots\ldots$; similarly we will now introduce substitutions of the letters $g_1, g_2 \ldots\ldots g_\kappa$ and agree that the same letter g_γ may indifferently be represented by g_γ or $l_2 g_\gamma$, $l_3 g_\gamma \ldots\ldots$ or $l_\lambda g_\gamma$. Then the symbol

$$\mathfrak{g}_\gamma = \begin{pmatrix} g_1 & , g_2 & , \ldots\ldots g_\kappa \\ g_1 g_\gamma, & g_2 g_\gamma, & \ldots\ldots g_\kappa g_\gamma \end{pmatrix} \tag{5}$$

represents a substitution between the κ letters $g_1, g_2 \ldots\ldots g_\kappa$, $g_\alpha g_\gamma$ being equivalent to g_β, if $g_\alpha g_\gamma = lg_\beta$. According to a theorem due to Jordan,* the κ substitutions

$$\mathfrak{g}_1, \mathfrak{g}_2, \ldots\ldots \mathfrak{g}_\kappa$$

* Jordan, l. c. No. 69; see besides, König: *Ueber rationale Functionen von n Elementen*, Math. Ann. Vol. 14, and especially Capelli: *Sopra l'isomorfismo dei gruppi di sostituzioni*, Giornale di Matematiche, Vol. 16, pg. 43.

form a regular group* $\mathfrak{G}$, *which is meriedrically isomorphic to* G, the λ substitutions

$$l_1 g_\gamma,\ l_2 g_\gamma,\ \ldots .\ l_\lambda g_\gamma$$

of G being coordinated ("zuordnen") with the substitution $\mathfrak{g}_\gamma$ of $\mathfrak{G}$.

In fact the group $\mathfrak{G}$ is identical with the group of those substitutions which undergo, under the action of the substitutions of G, the $\varkappa$ conjugate ("gleichberichtigt") values of a rational function $\phi\,(x_1 x_2 \ldots .)$ which remains unaltered by the substitutions of the subgroup L and no other.

Defining in an analogous way the symbol

$$\mathfrak{h}_\gamma = \begin{pmatrix} h_1 & , h_2 & , \ldots . h_\kappa \\ h_1 h_\gamma, & h_2 h_\gamma, & \ldots . h_\kappa h_\gamma \end{pmatrix} \tag{6}$$

as a substitution, we introduce the group

$$\mathfrak{H} = [\mathfrak{h}_1 = 1,\ \mathfrak{h}_2,\ \ldots .\ \mathfrak{h}_\kappa],$$

which is regular and meriedrically isomorphic to H, the μ substitutions

$$m_1 h_\gamma,\ m_2 h_\gamma,\ \ldots .\ m_\mu h_\gamma$$

of H being coordinated with the substitution $\mathfrak{h}_\gamma$ of $\mathfrak{H}$.

Now we replace in each of the $\varkappa$ multipliers $g_\gamma h_\gamma$ (3), the factor g_γ by the corresponding substitution $\mathfrak{g}_\gamma$, and the factor h_γ by the corresponding substitution $\mathfrak{h}_\gamma$, and obtain in this way a series of $\varkappa$ products,

$$\mathfrak{g}_1\mathfrak{h}_1 = 1,\ \mathfrak{g}_2\mathfrak{h}_2,\ \ldots .\ \mathfrak{g}_\kappa\mathfrak{h}_\kappa . \tag{7}$$

I say *these $\varkappa$ substitutions* (7) *form a group.* For if $\mathfrak{g}_\alpha\mathfrak{h}_\alpha$ and $\mathfrak{g}_\beta\mathfrak{h}_\beta$ be any two substitutions of the series (7), the series (3) will contain the two products $g_\alpha h_\alpha$ and $g_\beta h_\beta$, and the group I their product $g_\alpha g_\beta . h_\alpha h_\beta$, which we may reduce to the form $lm \times g_\gamma h_\gamma = l g_\gamma . m h_\gamma$, $g_\gamma h_\gamma$ being one of the multipliers (3). Hence we infer

$$g_\alpha g_\beta = l g_\gamma,\ h_\alpha h_\beta = m h_\gamma .$$

On account of the isomorphic relation between $\mathfrak{G}$ and G, the product $\mathfrak{g}_\alpha\mathfrak{g}_\beta$ in $\mathfrak{G}$ corresponds to the product $g_\alpha g_\beta$ in G; but on the other hand $\mathfrak{g}_\gamma$ corresponds to $l g_\gamma$; therefore since to every substitution of G corresponds but one single substitution of $\mathfrak{G}$, the equation $g_\alpha g_\beta = l g_\gamma$ implies $\mathfrak{g}_\alpha\mathfrak{g}_\beta = \mathfrak{g}_\gamma$, and likewise $\mathfrak{h}_\alpha\mathfrak{h}_\beta = \mathfrak{h}_\gamma$.

But $g_\gamma h_\gamma$ belonging to the series (3), the series (7) contains the product $\mathfrak{g}_\gamma\mathfrak{h}_\gamma = \mathfrak{g}_\alpha\mathfrak{g}_\beta . \mathfrak{h}_\alpha\mathfrak{h}_\beta = \mathfrak{g}_\alpha\mathfrak{h}_\alpha \times \mathfrak{g}_\beta\mathfrak{h}_\beta$, which shows that in fact the substitutions (7) form a group which we will denote by $\mathfrak{J}$.

* A substitution-group is said to be *regular*, according to Klein, if it is transitive and its order equals its degree.

This group is evidently *intransitive* and possesses the two systems of intransitivity,

$$g_1, g_2 \ldots . g_\kappa \text{ and } h_1, h_2 \ldots . h_\kappa,$$

and *its transitive constituents are the groups* $\mathfrak{G}$ and $\mathfrak{H}$.

Moreover $\mathfrak{J}$ is meriedrically isomorphic to I, the $\lambda\mu$ substitutions

$$l_\alpha g_\gamma . m_\beta h_\gamma \; (\alpha = 1, 2 \ldots . \lambda; \; \beta = 1, 2 \ldots . \mu)$$

of I corresponding to the substitution $\mathfrak{g}_\gamma \mathfrak{h}_\gamma$ of $\mathfrak{J}$; to unity in $\mathfrak{J}$ corresponds the subgroup J of I.

Finally the connection between the group $\mathfrak{J}$ and the multipliers (3) shows plainly that *each substitution of* $\mathfrak{G}$ (*and likewise each substitution of* $\mathfrak{H}$) *occurs only in one single substitution of* $\mathfrak{J}$.

5. *Conversion*: Let us now suppose *we choose at will the self-conjugate subgroups* L *and* M of the two given groups G and H resp., but such that their orders λ and μ satisfy the relation (4),

$$\frac{p}{\lambda} = \frac{q}{\mu} = \kappa,$$

and form the group J by multiplying their substitutions in all possible ways. Then we derive, as in No. 4, the regular groups $\mathfrak{G}$ and $\mathfrak{H}$ isomorphic to G and H resp. Finally, we suppose it possible to construct an intransitive group

$$\mathfrak{J} = [\mathfrak{g}_1\mathfrak{h}_1, \mathfrak{g}_2\mathfrak{h}_2 \ldots . \mathfrak{g}_\kappa\mathfrak{h}_\kappa]$$

with the transitive constituent groups $\mathfrak{G}$ and $\mathfrak{H}$, and such that each substitution of $\mathfrak{G}$ (and each substitution of $\mathfrak{H}$) occurs but in one single substitution of $\mathfrak{J}$.

Repeating, then, in reversed order, the conclusions of the last number, we easily find:

If in each substitution $\mathfrak{g}_\gamma\mathfrak{h}_\gamma$ of $\mathfrak{J}$ we replace $\mathfrak{g}_\gamma$ by any of its corresponding substitutions of G, g_γ, and $\mathfrak{h}_\gamma$ by any of its corresponding substitutions of H; h_γ, and multiply the $\lambda\mu$ substitutions of J by these κ products, $g_1h_1, g_2h_2 \ldots . g_\kappa h_\kappa$, the $\lambda\mu\kappa$ substitutions thus obtained form an intransitive group I whose transitive constituents are the given groups G and H.

Thus we have obtained the result announced in the beginning of this §: *The construction of the intransitive group I is indeed resolved into the construction of two intransitive groups which represent the two extreme types* of intransitive groups, viz. *the group J* in which the substitutions of the two constituent groups L and

M appear multiplied together in all possible ways, *and the group* $\mathfrak{J}$ in which each substitution of either of the constituent groups $\mathfrak{G}$ and $\mathfrak{H}$ appears multiplied only by one single substitution of the other constituent group.

§2.

Connection between Intransitive Groups and Isomorphism.

1. Before we pass to the construction of the group $\mathfrak{J}$, we must mention a theorem due to Netto, by which an intimate connection is established between intransitive groups and isomorphism. A group H is said to be *isomorphic, in the most general sense** of the word, to a group G, if it is possible to establish between the two groups a relation of the following character: With each substitution of G are coordinated one or several substitutions of H, and if $h_1, h_2 \ldots . h_\nu$ be all the substitutions *coordinated with a substitution* g, *and* $h'_1, h'_2 \ldots . h'_{\nu'}$ all the substitutions coordinated with any other g', then all the products, $h_\alpha h'_{\alpha'}$ $(\alpha = 1, 2 \ldots . \nu;\ \alpha' = 1, 2 \ldots . \nu')$ and no other substitutions of H, shall be coordinated with the product gg'. Besides, it is supposed that all the substitutions of H are engaged in this coordination.

From this definition *follows* that reciprocally the group G is isomorphic to H, so that the isomorphism between the two groups is perfectly mutual.

The holoedric and the meriedric isomorphism, as defined by Jordan, are special cases of this general isomorphism, which has been called by Netto *mutually meriedric* ("gegenseitig mehrstufig").

Now Netto's theorem† is this:

Suppose the two isomorphic groups G and H to operate upon different letters; if, then, each substitution of G is successively multiplied by all its corresponding substitutions of H, the products will form an intransitive group with the constituent groups G and H.

And conversely: If an intransitive group I with the constituent groups G and H be given, and we coordinate with each substitution of G all those substitutions of H with which it appears multiplied in the substitutions of I, then the relation thus established between the two groups will be isomorphic.

2. *Every intransitive group may consequently be considered as defining an isomorphic relation between two groups*, and any theorem on intransitive groups

---

*Netto: Substitutionentheorie, §93. †Ib. l. c. §93.

may be interpreted as a theorem on isomorphism. For instance, denoting by O_γ the system of λ substitutions, $l_1 g_\gamma$, $l_2 g_\gamma \ldots . l_\lambda g_\gamma$, and by Ω_γ the system of μ substitutions, $m_1 h_\gamma$, $m_2 h_\gamma \ldots . m_\mu h_\gamma$, we may express the results of §§1, 3 in this form:

If two groups G and H are isomorphic, the substitutions of G can be distributed into a number of systems

$$O_1, O_2 \ldots, O_\kappa,$$

and those of H in an *equal* number of corresponding systems,

$$\Omega_1, \Omega_2, \ldots . \Omega_\kappa$$

such that any substitution of O_γ is coordinated with all the substitutions of the corresponding system Ω_γ and with no other, and, vice versa, any substitution of Ω_γ with all the substitutions of O_γ .

But this is exactly what Capelli,* who has first considered this general kind of isomorphism, *assumes in his definition*, so that by our developments the definitions of Capelli and Netto, though apparently different, are found to be identical.

3. If we apply Netto's theorem to the intransitive group $\mathfrak{J}$ of §1 and remember that in $\mathfrak{J}$ each substitution of $\mathfrak{G}$ appears multiplied only by one substitution of $\mathfrak{H}$ and vice versa, we see that the group $\mathfrak{J}$ defines, between $\mathfrak{G}$ and $\mathfrak{H}$, a holoedric isomorphism, in which the substitution $\mathfrak{g}_\gamma$ of $\mathfrak{G}$ is coordinated with that substitution $\mathfrak{h}_\gamma$ of $\mathfrak{H}$ with which $\mathfrak{g}_\gamma$ appears multiplied in the substitution $\mathfrak{g}_\gamma \mathfrak{h}_\gamma$ of $\mathfrak{J}$.

§3.

Holoedric Isomorphic Relation of a Regular Group to itself.

1. In order to be in accordance with the usual notations, we will write henceforth G and H instead of $\mathfrak{G}$ and $\mathfrak{H}$, and denote the letters upon which the substitutions of G and H operate by $x_1, x_2 \ldots . x_r$ resp. $y_1, y_2 \ldots . y_r$. Since the two groups are supposed to be *regular and holoedrically isomorphic*, they must be, according to a theorem of Jordan's,† *altogether identical except*

* Capelli, l. c. pg. 33. Starting from this definition, Capelli proves that the different systems O_γ contain the same number λ of substitutions, and the different systems Ω_γ the same number μ of substitutions, and thus finds the relation (4), $\frac{p}{\lambda} = \frac{q}{\mu}$.

† Jordan, l. c. No. 70, 72, and Netto, l. c. §90.

the notation of the letters upon which they operate. Therefore there must exist a certain permutation of the $x : x_{i_1}, x_{i_2} \ldots . x_{i_r}$, such that each substitution h_a of H becomes identical with the corresponding substitution g_a of G, if we replace, *within the cycles of* h_a, the letter y_1 by x_{i_1}, y_2 by x_{i_2}, and so on; or denoting by u the substitution

$$u = \begin{pmatrix} x_1, & x_2 \ldots . & x_r, & y_1, & y_2 & \ldots . & y_r \\ y_1, & y_2 \ldots . & y_r, & x_{i_1}, & x_{i_2} & \ldots . & x_{i_r} \end{pmatrix} \tag{8}$$

we must have, between any two corresponding substitutions g_a and h_a, the relation

$$g_a = u^{-1} h_a u, \qquad \alpha = 1, 2 \ldots . r \tag{9}$$

and between the groups themselves,

$$G = u^{-1} H u. \tag{10}$$

If there exist still another holoedric isomorphic relation between G and H, there will exist another substitution u' such that

$$G = u'^{-1} H u';$$

u' can be reduced to the form

$$u' = ut,$$

where t is a substitution between the x which transforms G into itself,

$$t^{-1} G t = G. \tag{11}$$

For from $\quad u^{-1} H u = G$ and $u'^{-1} H u' = G$

follows $\quad u'^{-1} u G u^{-1} u' = G,$

or if we put $u^{-1} u' = t$,

$$t^{-1} G t = G$$

and $\quad u' = ut.$

We can write $\quad u = v\tau, \; u' = v'.\tau,$

where

$$\tau = (x_1, y_1)(x_2, y_2) \ldots . (x_r, y_r) \tag{12}$$

and v, v' are substitutions of the letters y only; then we see that

$$t = \tau^{-1} (v^{-1} v') \tau$$

is a substitution between the x only.

The equation $t^{-1} G t = G$ defines a holoedric isomorphic relation of G to itself, in which any substitution g is coordinated with its transformed $t^{-1} g t$.

Thus *the construction of the intransitive group I is at last reduced to the problem: To find all possible holoedric isomorphic relations of a regular group to itself.*

2. The substitutions t which satisfy the relation $t^{-1}Gt = G$ form a *group* T, which is *the largest group with the letters* $x_1, x_2 \ldots . x_r$ *in which the group* G *is contained as a self-conjugate subgroup.**

The group T always contains substitutions which are *commutative* not only to the whole group G, but *to each of its substitutions*. These substitutions form a group which has been studied by Jordan;† it is itself regular and of the same order as G and can be derived from it by an algorithm indicated by Jordan. We denote this group by

$$S = [s_1 = 1, s_2, \ldots . s_r].$$

S being a subgroup of T, we can write the substitutions of T in the form

$$s_\alpha t_\beta, \ \alpha = 1, 2 \ldots . r, \ \beta = 1, 2 \ldots . \rho.$$

Two substitutions of T with the same factor t_β will transform the group G exactly in the same way and therefore lead to the same isomorphic relation of G to itself; for

$$(st_\beta)^{-1} g \, (st_\beta) = t_\beta^{-1} (s^{-1} gs) \, t_\beta,$$

which is equal to $t_\beta^{-1} g t_\beta$, since $s^{-1}gs$ is supposed to be $= g$.

To obtain all the *distinct* isomorphic relations it is therefore sufficient to know a complete system of multipliers, $t_1, t_2 \ldots . t_\rho$.

The problem to determine the group T for a given regular group G has been completely solved by Jordan‡ in the case where G is the group of the arithmetical substitutions

$$|z_1, z_2 \ldots . z_n; \ z_1 + \alpha_1, z_2 + \alpha_2, \ldots . z_n + \alpha_n|,$$
$$\alpha_1 = 0, 1 \ldots . m-1, \ \alpha_2 = 0, 1 \ldots . m-1, \ldots . \alpha_n = 0, 1 \ldots . m-1.$$

In this case S is identical with G and the group T is the *linear group of the degree* m^n, which is generated by combining the given group with the group of the geometrical substitutions

$$|z_1, z_2 \ldots . z_n; \ a_{11}z_1 + a_{12}z_2 + \ldots ., \ a_{21}z_1 + a_{22}z_2 + \ldots .; \ \ldots . a_{n_1}z_1 + a_{n_2}z_2 + \ldots .|,$$

the determinant $|a_{\alpha\beta}|$ being prime to m.

Here the group of the geometrical substitutions form a complete system of multipliers $t_1, t_2 \ldots . t_\rho$.

---

* Netto, l. c. §78.

† Jordan, l. c. No. 75. See also Frattini: *I gruppi transitivi di sostituzioni dell' istesso ordine e grado.* Atti della R. Acc. dei Lincei, Memorie, 1883.

‡ Jordan, l. c. No. 19, and Netto, l. c. §137.

3. The isomorphic relation of a group G to itself can be found in a different way without recurring to the group T, provided we know a system of *independent generating substitutions** $a, b, c \dots$ of G and the fundamental relations between them. For if

$$\begin{aligned} a' &= \phi(a, b, c \dots), \\ b' &= \psi(a, b, c \dots), \\ c' &= \chi(a, b, c \dots)\dagger \\ &\dots\dots\dots\dots \end{aligned} \tag{13}$$

be the substitutions which are coordinated with $a, b, c \dots$ resp., then exactly the same relations will exist between the $a', b', c' \dots$ as between the $a, b, c \dots$, and therefore the $a', b', c' \dots$ will constitute another system of generating substitutions for the group G. Conversely, if $a', b', c' \dots$ be another system of independent substitutions satisfying the same fundamental relations (and no other besides), and if we coordinate a' with a, b' with b, c' with c, and so on, and with each product of the $a, b, c \dots$ the similar product of the $a', b', c' \dots$, then we shall have established a holoedric isomorphism of the group G with itself.

For instance, the *cyclic group* of the order n can be generated by a single substitution a, satisfying the relation $a^n = 1$, and no other relation $a^{n'} = 1$ where $n' < n$. The same conditions are satisfied by $a' = a^\mu$, provided μ be prime to n. Therefore we obtain a holoedric isomorphic relation of the cyclic group to itself by coordinating a^α with $a^{\mu\alpha}$, $\alpha = 0, 1, \dots n-1$, and there are $\phi(n)$ different isomorphic relations.

We may even use this method to determine backwards the group T. For by comparing the generating substitutions $a, b, c \dots$ with their corresponding substitutions $a', b', c' \dots$ we can easily find the substitutions t_β of No. 2, and by combining these with the group S we obtain the group T.

Example: The *symmetrical group of three letters* can be generated by two substitutions a, b, satisfying the relations

$$a^3 = 1, \ b^2 = 1, \ ba = a^2 b;$$

the group is then

$$1, a, a^2, b, ab, a^2 b.$$

* Compare for this number, Cayley, *On the Theory of Groups*, Phil. Mag., 4th series, Vol. 7, 18, and *American Journal of Mathematics*, Vol. 1; and Dyck, *Gruppentheoretische Studien*, Math. Ann., Vol. 22.

† The $\phi, \psi, \chi \dots$ represent products $a^\alpha b^\beta c^\gamma \dots a^{\alpha'} b^{\beta'} c^{\gamma'} \dots$

If we choose for a' any of the substitutions of the third order (a or a^2), for b' any of the substitutions of the second order (b, or ab, or a^2b), it is easily seen that a', b' satisfy the same relations

$$a'^3 = 1\,,\ b'^2 = 1\,,\ b'a' = a'^2b',$$

and no other, and we have therefore six different isomorphic relations of our group to itself. The regular form* of our group is

$$\begin{aligned}1\,;\ a &= (x_1x_2x_3)(x_4x_5x_6)\,;\quad a^2 = (x_1x_3x_2)(x_4x_6x_5)\,;\ b = (x_1x_4)(x_2x_6)(x_3x_5)\,;\\ ab &= (x_1x_5)(x_2x_4)(x_3x_6)\,;\ a^2b = (x_1x_6)(x_2x_5)(x_3x_4)\,.\end{aligned}$$

To find the substitution t, for instance, for the isomorphic relation defined by $a' = a$, $b' = ab$, we have to determine a substitution which, applied within the cycles of a and b, changes

$$(x_1x_2x_3)(x_4x_5x_6)$$

into itself, and

$$(x_1x_4)(x_2x_6)(x_3x_5) \text{ into } (x_1x_5)(x_2x_4)(x_3x_6)\,;$$

evidently $(x_1x_2x_3)$ is such a substitution. In this way we find corresponding to the six isomorphic relations, the six substitutions,

$$\begin{aligned}&t_1 = 1\,,\ t_2 = (x_1x_2x_3)\,,\ t_3 = (x_1x_3x_2)\,,\\ &t_4 = (x_5x_6)(x_2x_3)\,,\ t_5 = (x_5x_6)(x_3x_1)\,,\ t_6 = (x_5x_6)(x_1x_2)\,.\end{aligned}$$

On the other hand the group S is easily found to be

$$\begin{aligned}1\,;\ &(x_1x_2x_3)(x_4x_6x_5)\,,\ (x_1x_3x_2)(x_4x_5x_6)\,,\ (x_1x_4)(x_2x_5)(x_3x_6)\,,\\ &(x_1x_5)(x_2x_6)(x_3x_4)\,,\ (x_1x_6)(x_2x_4)(x_3x_5)\,.\end{aligned}$$

These combined with the six t give the group T, which is of the order 36, and is made up of the positive ("gerade") substitutions contained in the most general imprimitive group with the two systems of imprimitivity,

$$x_1,\ x_2,\ x_3 \text{ and } x_4,\ x_5,\ x_6.$$

This is then the largest group with the letters $x_1, x_2 \ldots . x_6$ in which G is contained as a self-conjugate subgroup.

4. As an *example of the construction of intransitive groups*, we propose to find all the intransitive groups with the two systems of intransitivity,

$$x_1,\ x_2,\ x_3,\ x_4 \text{ and } y_1,\ y_2,\ y_3,\ y_4,$$

---

*That is to say, the regular group which is holoedrically isomorphic to the given group; see Dyck, l. c. §6.

whose transitive constituents are the *alternate group* G_{12} of the letters x_1, x_2, x_3, x_4 and the alternate group H_{12} of the letters y_1, y_2, y_3, y_4.

The group G_{12} can be generated by two substitutions a and c, satisfying the relations

$$a^2 = 1, \; c^3 = 1, \; (ac)^3 = 1. \tag{14}$$

Introducing, for shortness, the notation

$$b = cac^2,$$

the group G_{12} may be exhibited in the following table:

$$\begin{array}{llll} 1, & a\;, & b\;, & ab\;, \\ c\;, & ac\;, & bc\;, & abc\;, \\ c^2, & ac^2, & bc^2, & abc^2, \end{array} \tag{15}$$

whose first line represents the "Four-group" ("Vierergruppe"), which shall be denoted by G_4, and which is, besides G_{12} itself and $G_1 = 1$, the only self-conjugate subgroup of G_{12}.

We may choose, for instance,

$$a = (x_1x_2)(x_3x_4), \; c = (x_1x_2x_3),$$

and we obtain all the possible systems a', c' of generating substitutions which satisfy the same fundamental relations, by choosing for a' any of the three substitutions of the second order, a, b, ab, and for c' any of the eight substitutions of the third order,

$$c, \; ac, \; bc, \; abc; \; c^2, \; ac^2, \; bc^2, \; abc^2.$$

For since c' does not belong to the subgroup G_4, whereas a' does, $a'c'$ cannot belong to G_4 and must therefore be one of the eight substitutions of the third order, therefore we have

$$a'^2 = 1, \; c'^3 = 1, \; (a'c')^3 = 1. \tag{16}$$

And there can exist *no other relation* between a' and c' independent of these. For any such relation could, by means of (16), be reduced to the form: one of the products of the table (15), marked with dashes, equal to unity (b' denoting $c'a'c'^2$). Let us for instance suppose we had besides (16) the relation $a'b'c' = 1$; now $a'b'c'$ is conjugate ("gleichberechtigt") in G_{12} with c', since, on account of (16), $a'b'c' = a'^{-1}c'a'$; therefore the relation $a'b'c' = 1$ implies* $c' = 1$, which is in contradiction with our assumption about c'. Since the substitutions a, b, ab are conjugate in G_{12}, and likewise the substitutions of the second line of (15), and

* Compare for these conclusions Dyck, l. c. §3.

finally those of the third line, we see that any relation between a' and c', independent of (16), would imply either $a'=1$, or $c'=1$ or $c'^2=1$.

There exist therefore $3.8=24$ different systems of generating substitutions satisfying the relations (14) and no other.

Denoting the generating substitutions of H_{12} by d, f, we have

$$d^2=1,\ f^3=1,\ (df)^3=1.$$

And putting again $e=fdf^2$, the group H_{12} may be exhibited in the table

$$\begin{array}{llll} 1\ , & d\ , & e\ , & de\ , \\ f\ , & df\ , & ef\ , & def\ , \\ f^2, & df^2, & ef^2, & def^2, \end{array} \tag{17}$$

whose first line shall be denoted by H_4.

On account of the relation (4) we can choose the self-conjugate subgroups L, M of §1 in three different ways: either G_{12}, $H_{12}\,(\varkappa=1)$, or G_4, $H_4\,(\varkappa=3)$, or G_1, $H_1\,(\varkappa=12)$.

a). $$\varkappa=1;\ L=G_{12},\ M=H_{12}.$$

I is of the order 144, and is obtained by multiplying every substitution of G_{12} by every substitution of H_{12}.

b). $$\varkappa=3;\ L=G_4,\ M=H_4.$$

The multipliers g_1, g_2, g_3 of §1, 3 are here:

$$g_1=1,\ g_2=c,\ g_3=c^2,$$

hence

$$\mathfrak{g}_1=1,$$

$$\mathfrak{g}_2=\begin{pmatrix} g_1 & , g_2 & , g_3 \\ g_1g_2, & g_2g_2, & g_3g_2 \end{pmatrix}=(g_1, g_2, g_3)=\mathfrak{g},$$

$$\mathfrak{g}_3=\begin{pmatrix} g_1 & , g_2 & , g_3 \\ g_1g_3, & g_2g_3, & g_3g_3 \end{pmatrix}=(g_1, g_3, g_2)=\mathfrak{g}^2,$$

$$\mathfrak{G}=[1,\ \mathfrak{g},\ \mathfrak{g}^2].$$

In the isomorphism between $\mathfrak{G}$ and G_{12}, 1 is coordinated with the first line of the table (15), $\mathfrak{g}$ with the second, $\mathfrak{g}^2$ with the third.

Further,

$$h_1=1,\ h_2=f,\ h_3=f^2,$$

$$\mathfrak{h}_1=1,\ \mathfrak{h}_2=(h_1, h_2, h_3)=\mathfrak{h};\ \mathfrak{h}_3=(h_1, h_3, h_2)=\mathfrak{h}^2,$$

$$\mathfrak{H}=[1,\ \mathfrak{h},\ \mathfrak{h}^2].$$

The substitution 1 of $\mathfrak{H}$ is coordinated with the first line of the table (17), $\mathfrak{h}$ with the second, $\mathfrak{h}^2$ the third.

There exist two intransitive groups $\mathfrak{J}$ of the third order with the transitive constituents $\mathfrak{G}$ and $\mathfrak{H}$ (§3, 3), viz.

$$1\,,\ \mathfrak{g}\mathfrak{h}\,,\ \mathfrak{g}^2\mathfrak{h}^2,$$

and

$$1\,,\ \mathfrak{g}\mathfrak{h}^2,\ \mathfrak{g}^2\mathfrak{h}.$$

Consequently we obtain *two intransitive groups I of the order* 48: the first by multiplying every substitution of the first line of (15) by every substitution of the first line of (17), every one of the second by every one of the second, every one of the third by every one of the third; the second group I by multiplying every substitution of the first line of (15) by every substitution of the first line of (17), every one of the second by every one of the third, every one of the third by every one of the second.

c). $$\varkappa = 12;\ L = 1,\ M = 1.$$

Here $\mathfrak{G}$ is nothing but the regular form of the group G_{12}, $\mathfrak{H}$ the regular form of the group H_{12}. The 24 systems of generating substitutions of G_{12} define as many holoedric isomorphic relations of G_{12} (and therefore also of $\mathfrak{G}$) to itself, and consequently we obtain 24 *groups I of the order* 12, all contained in the table:

$$\begin{array}{llll}
1 & ,\ a'.d & ,\ b'.e & ,\ a'b'.de, \\
c'.f & ,\ a'c'.df & ,\ b'c'.ef & ,\ a'b'c'.def, \\
c'^2.f^2, & a'c'^2.df^2, & b'c'^2.ef^2, & a'b'c'^2.def^2,
\end{array}$$

if we replace a', c' successively by the 24 different systems of generating substitutions.

§4.

Some Applications to the Construction of Transitive Groups.

1. In a note published in the Mathematische Annalen,* Cayley proves a theorem which is closely connected with our subject, and which, in our notations, may be expressed thus:

"Let $G = [g_1, g_2 \ldots g_r]$ be a substitution-group with the letters $x_1, x_2 \ldots,$ whose substitutions are *commutative each to each*, and let h_α be the same substitution as g_α but operating upon different letters $y_1, y_2 \ldots,$ and let τ denote the substitution

$$\tau = (x_1y_1)(x_2y_2)(x_3y_3)\ \ldots\ ,$$

* Cayley, *A Theorem on Groups*, Math. Ann., Vol. 13.

then the $2r$ substitutions

$$\begin{array}{llll} g_1h_1^m & , g_2h_2^m ; & \ldots\ldots & g_rh_r^m, \\ g_1h_1^m.\tau, & g_2h_2^m\tau, & \ldots\ldots & g_rh_r^m.\tau \end{array}$$

will always form a group, if

$$m^2 \equiv 1 \qquad (\text{mod. } r)."$$

The first line of this group is an intransitive group of the special class considered in the last §, and we propose therefore to apply the developments of §3 to the problem:

Suppose the two regular groups G and H of the order r of §3, 1 to be identical, but operating upon different letters x resp. y; h_α shall denote the same substitution of $y_1, y_2 \ldots\ldots y_r$ which g_α denotes of the $x_1, x_2, \ldots\ldots x_r$. Let then

$$I = [g_1h_{i_1}, g_2h_{i_2} \ldots\ldots g_rh_{i_r}]$$

be an intransitive group of the same order r with the transitive constituents G and H; $i_1, i_2, \ldots\ldots i_r$ is then a certain permutation of $1, 2 \ldots\ldots r$ and there exists, according to §3, 1, a substitution u such that

$$u^{-1}h_{i_\alpha}u = g_\alpha, \ \alpha = 1, 2 \ldots\ldots r. \tag{18}$$

Now we multiply the substitutions of I by the substitution

$$\tau = (x_1y_1)(x_2y_2) \ldots\ldots (x_ry_r),$$

it is required to find the conditions that the $2r$ substitutions

$$\begin{array}{llll} g_1h_{i_1} & , g_2h_{i_2} & \ldots\ldots & g_rh_{i_r}, \\ g_1h_{i_1}.\tau, & g_2h_{i_2}.\tau & \ldots\ldots & g_rh_i\ .\tau \end{array} \tag{19}$$

form a group.

If they do form a group Q, this group will be imprimitive with the two systems of imprimitivity $x_1, x_2 \ldots\ldots x_r$ and $y_1, y_2 \ldots\ldots y_r$, and I will consist of all those substitutions of Q which do not interchange the systems, and therefore I will be a self-conjugate* subgroup of Q, and therefore

$$\tau^{-1}I\tau = I, \tag{20}$$

and this condition is sufficient, since then the two groups I and $[1, \tau]$, which contain no common substitution besides 1, are interchangeable among each other.†

* See Netto, l. c. §72.

† See Serret, Cours d'Algèbre, No. 435.

From (20) follows that $\tau^{-1}I\tau$ and I must possess the same constituent groups, therefore $\tau^{-1}H\tau = G$; τ and u being two substitutions which transform H into G, they must, according to §3, 1, be connected by an equation

$$u = \tau t, \tag{21}$$

t being commutative to G. Remembering, then, that according to the adopted notation

$$\tau^{-1}h_{i_\alpha}\tau = g_{i_\alpha},$$

(18) becomes
$$t^{-1}g_{i_\alpha}t = g_\alpha, \quad \alpha = 1, 2 \ldots . r. \tag{22}$$

On the other hand, $\tau^{-1}g_\alpha h_{i_\alpha}\tau$, which is equal to $\tau^{-1}g_\alpha\tau . \tau^{-1}h_{i_\alpha}\tau = g_{i_\alpha}h_\alpha$ belongs again to I (20), and therefore g_{i_α} and h_α must satisfy (18),

$$u^{-1}h_\alpha u = g_{i_\alpha},$$

or
$$t^{-1}g_\alpha t = g_{i_\alpha}, \quad \alpha = 1, 2 \ldots . r. \tag{23}$$

This equation combined with (22) gives

$$t^{-2}g_\alpha t^2 = g_\alpha, \quad \alpha = 1, 2 \ldots . r. \tag{24}$$

If, conversely, t satisfy this condition and we choose $h_{i_\alpha} = \tau t g_\alpha t^{-1}\tau^{-1}$, then we find $\tau^{-1}I\tau = I$. We see therefore that the square of the substitution t must belong to the group denoted in §3, 2 by S. For instance, in the case of the group of the arithmetical substitutions mentioned in §3, 2, we find easily for the substitution (see pg. 23):

$$t = |z_1, z_2 \ldots z_n;\ a_{11}z_1 + a_{12}z_2 + \ldots,\ a_{21}z_1 + a_{22}z_2 + \ldots,\ \ldots\ a_{n1}z_1 + a_{n2}z_2 + \ldots|$$

the condition

$$\sum_{\beta=1}^{n} a_{\alpha\beta}a_{\beta\gamma} \equiv \begin{cases} 0, & \text{if } \gamma \gtrless \alpha \\ 1, & \text{if } \gamma = \alpha \end{cases} \pmod{m}.$$

The relation (24) shows that the isomorphic relation of G to itself as defined by the equation

$$t^{-1}Gt = G,$$

possesses the *character of an involution*, that is to say, if g_β in the transformed group is coordinated with g_α in the original group, then reciprocally g_β in the original group will be coordinated with g_α in the transformed group.

Applying this to the generating substitutions $a, b, c \ldots.$ of §3, 3, we see that the transformation (13) must possess the period 2, that is,

$$\begin{aligned} a &= \phi(a', b', c' \ldots.), \\ b &= \psi(a', b', c' \ldots.), \\ c &= \chi(a', b', c' \ldots.). \\ &\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Let us now return to Cayley's theorem and suppose that any two substitutions of G are commutative to each other. Then, according to a theorem of Kronecker's,* G can be generated by a series of substitutions $a, b, c \ldots$, commutative each to each and of the orders r_1, r_2, r_3 resp., the integers $r_1, r_2, r_3 \ldots$ forming a series in which *each integer is divisible by the following*, and besides their product equals the order of G:

$$r = r_1 . r_2 . r_3 \ldots.$$

By coordinating each substitution g_α with g_α^m, we always obtain a holoedric isomorphic relation of G to itself, if m be prime to r, since $(g_\alpha g_\beta)^m = g_\alpha^m g_\beta^m$ in this case. The corresponding transformation (13) of the generating substitutions is

$$a' = a^m, \; b' = b^m, \; c' = c^m, \ldots.,$$

and this has the period 2, then and only then, when

$$a^{m^2} = a, \; b^{m^2} = b, \; c^{m^2} = c, \ldots.,$$

which implies the only condition,

$$m^2 \equiv 1 \; (\text{mod. } r_1),$$

since $r_2, r_3, \ldots.$ are divisors of r.

This congruence includes Cayley's theorem, since r is divisible by r_1.

2. We conclude with some general remarks on the construction of groups.

The fundamental problem of the abstract theory of groups is, *to construct all the groups of a given order;* groups which are holoedrically isomorphic may be considered as essentially identical in this research.

Now all possible groups of a given order r may be divided into *two classes:*

The first class contains all those groups which are *holoedrically isomorphic with intransitive groups whose transitive constituents are all of a smaller order than r.*

---

* Kronecker, Berliner Monatsberichte, 1870, and Netto, l. c. §133.

The second class contains all those groups for which no such isomorphism exists.

All the groups of the first class can be obtained by the method developed in this paper, provided all the groups of a smaller order than r have been previously determined, and thus the problem is reduced to the construction of the groups of the second class.

Examples:

1). $r = 4$. There are two groups,

α). $$1, a, a^2, a^3; \ a^4 = 1,$$

which belongs to the second class, and

β). $$1, a, b, ab; \ a^2 = 1, \ b^2 = 1, \ ba = ab,$$

which belongs to the first class, since we may choose

$$a = (x_1x_2), \ b = (y_1y_2).$$

2). $r = 6$. There are two groups,

α). $$1, a, a^2, a^3, a^4, a^5; \ a^6 = 1$$

belongs to the first class and becomes identical with the intransitive group

$$b = (x_1x_2), \ c = (y_1y_2y_3),$$
$$1, c, c^2, b, bc, bc^2,$$

if we put $a = bc$, which is indeed of the sixth order.

β). The group
$$1, a, a^2, b, ab, a^2b,$$
$$a^3 = 1, \ b^2 = 1, \ ba = a^2b,$$

belongs to the second class, but can be obtained by Cayley's theorem. For if we put

$$c = (x_1x_2x_3), \ d = (y_1y_2y_3), \ \tau = (x_1y_1)(x_2y_2)(x_3y_3),$$

the group
$$1, cd^2, c^2d,$$
$$\tau, cd^2\tau, c^2d\tau$$

becomes identical with the given group if we write

$$a = cd^2, \ b = \tau.$$

3). $r = 8$. There exist five different groups enumerated by Cayley in the Phil. Mag. (4th series, Vol. 7, 18). Two of them belong to the first class.

In the group

$$a^4 = 1\,,\ b^2 = 1\,,\ ba = ab$$

we may choose $\quad a = (x_1x_2x_3x_4)\,,\ b = (y_1y_2)\,,$

and in the group $\quad a^2 = 1\ ,\ b^2 = 1\ ,\ c^2 = 1\,,$

$$ab = ba\,,\ ac = ca\,,\ bc = cb$$

we may choose $\quad a = (x_1x_2)\,,\ b = (y_1y_2)\,,\ c = (z_1z_2)\,.$

Finally, the group $\quad a^4 = 1\,,\ b^2 = 1\,,\ ab = ba^3$

belongs to the second class, but can be obtained by Cayley's theorem. For if we put

$$c = (x_1x_2x_3x_4)\,,\ d = (y_1y_2y_3y_4)\,,\ \tau = (x_1y_1)(x_2y_2)(x_3y_3)(x_4y_4)\,,$$

the group $\quad 1\,,\ cd^3\ ,\ c^2d^2\ ,\ c^3d\,,$

$$\tau\,,\ cd^3\tau\,,\ c^2d^2\tau\,,\ c^3d\tau$$

becomes identical with the given group if we write

$$a = cd^3,\ b = \tau.\text{*}$$

ORANGE, N. J., September, 1888.

---

* I avail myself of this opportunity to add a reference to a previous paper "On binary sextics with linear transformations into themselves" (this Journal, Vol. X, pg. 47): Mr. Wiltheiss has called my attention to a paper of his (Math. Ann., Vol. 21, pg. 398) which had escaped my notice, and in which he deals with the determination of those systems of hyperelliptic ϑ-moduli for which there exists a complex multiplication. It is easy to prove *a priori* that for the case of the transformation of the first degree (for which Mr. Wiltheiss gives a complete table) these systems of ϑ-moduli must be identical with those determined in the third section of my paper, and so I could have made use of Mr. Wiltheiss's results and determined afterwards the order in which these systems of ϑ-moduli are to be coordinated with the binary sextics, by considering the isomorphism which exists between the group of the linear transformation of the variables z_1, z_2 and the group of the linear transformation of the ϑ-moduli. But still the method employed in my paper has the advantage of showing directly the connection between the binary sextic and the corresponding ϑ-moduli. This method has, by the by, been first employed by Mr. Poincaré in a similar research.